Evropský sbor pro ochranu osobních údajů

Stanovisko sboru (čl. 70 odst. 1 písm. b))

Čl. 70 1 b

Stanovisko 23/2018 k návrhům Komise týkajícím se evropských předávacích a uchovávacích příkazů pro elektronické důkazy v trestních věcech (čl. 70 odst. 1 písm. b)

přijaté dne 26. září 2018

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. b) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,

PŘIJAL TOTO ROZHODNUTÍ:

Úvod

V dubnu 2018 předložila Komise návrh nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech a návrh směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení. Uvedené dva návrhy COM(2018) 225 final a COM(2018) 226 final se vzájemně doplňují. Celkovým cílem, který Komise sleduje, je zlepšit spolupráci mezi orgány členských států a poskytovateli služeb, včetně těch se sídlem v zemích mimo EU, a navrhnout řešení problému určení a vymáhání pravomoci v kyberprostoru.

Zatímco návrh nařízení předpokládá pravidla a postupy použitelné na vydávání uchovávacích a předávacích příkazů a jejich doručování poskytovatelům služeb elektronické komunikace, jakož i jejich vymáhání od poskytovatelů, návrh směrnice stanoví minimální pravidla pro ustanovení právního zástupce poskytovatelů služeb, kteří nejsou usazeni v EU.

V listopadu 2017[1], dříve než Komise předložila jakoukoli předlohu návrhu, připomenula pracovní skupina zřízená podle článku 29 (WP29) nutnost zajistit, aby byl každý legislativní návrh v plném souladu zejména se stávajícím *acquis* EU o ochraně osobních údajů, jakož i s unijním právem a judikaturou obecně.

WP 29 varovala zejména před omezením práv na ochranu osobních údajů a soukromí s ohledem na údaje zpracovávané poskytovateli telekomunikací a služeb informační společnosti, zvláště jsou-li dále zpracovávány donucovacími orgány, připomenula nutnost zajistit soulad všech nástrojů EU se stávající Budapešťskou úmluvou Rady Evropy o kyberkriminalitě a se směrnicí EU o evropském vyšetřovacím příkazu a doporučila vyjasnit příslušná procesní pravidla, kterými se řídí přístup k elektronickým důkazům na vnitrostátní úrovni a úrovni EU, aby se zajistilo, že nový nástroj neudělí orgánům nové pravomoci, které by na vnitrostátní úrovni neměly. Kromě těchto obecných připomínek se WP 29 vyjádřila k legislativním možnostem zvažovaným v té době Komisí ohledně kategorií dotčených údajů a odpovídajících záruk pro přístup k nim, k možnosti řešit předávací příkazy/žádosti s cílem donutit poskytovatele služeb, aby poskytli údaje nacházející se mimo EU, a k hmotněprávním a procesním podmínkám nezbytných záruk k ohraničení přímého přístupu k údajům.

Nyní, když má k dispozici konkrétní návrhy týkající se elektronických důkazů, chce Evropský sbor pro ochranu osobních údajů poskytnout podrobnější analýzu navrhovaných právních nástrojů z hlediska ochrany osobních údajů.

[1] Viz prohlášení pracovní skupiny zřízené podle článku 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Právní základ návrhu nařízení (článek 82 Smlouvy o fungování Evropské unie)

Navrhovaným právním základem návrhu nařízení o elektronických důkazech je čl. 82 odst. 1 Smlouvy o fungování Evropské unie (SFEU) týkající se justiční spolupráce v trestních věcech, který stanoví:

> „1. Justiční spolupráce v trestních věcech je v Unii založena na zásadě vzájemného uznávání rozsudků a soudních rozhodnutí a zahrnuje sbližování právních předpisů členských států v oblastech uvedených v odstavci 2 a v článku 83.
>
> Evropský parlament a Rada přijímají řádným legislativním postupem opatření, která mají za cíl:
>
> a) stanovit pravidla a postupy pro zajištění uznávání všech forem rozsudků a soudních rozhodnutí v celé Unii;
>
> b) předcházet střetům příslušnosti mezi členskými státy a řešit je;
>
> c) podporovat další vzdělávání soudců a soudních zaměstnanců;
>
> d) usnadňovat spolupráci mezi justičními nebo obdobnými orgány členských států v rámci trestního řízení a výkonu rozhodnutí.“

Jak Komise zdůrazňuje v posouzení dopadů připojeném k návrhům, „čl. 82 odst. 1 stanoví, že justiční spolupráce v trestních věcech je založena na zásadě vzájemného uznávání. Tento právní základ by se vztahoval na možné právní předpisy o přímé spolupráci s poskytovateli služeb, ve kterých by orgány ve vydávajícím členském státě přímo oslovily subjekt (poskytovatele služeb) ve vykonávajícím státě a dokonce mu ukládaly povinnosti. To by do vzájemného uznávání zavedlo nový rozměr přesahující tradiční justiční spolupráci v Unii doposud založenou na postupech zahrnujících dva justiční orgány, jeden ve vydávajícím státě a druhý ve vykonávajícím státě“ (zvýraznění doplněno).

Vzhledem k tomu, že použití tohoto právního základu v rámci přímých žádostí mezi orgány veřejné moci a soukromými subjekty je novinkou, Evropský sbor pro ochranu osobních údajů vyjadřuje politování nad tím, že Komise neposkytla žádnou další analýzu ani posouzení.

Jak již zdůraznila pracovní skupina ve svém předchozím prohlášení, Evropský sbor pro ochranu osobních údajů nadále upozorňuje na své pochybnosti ohledně vhodnosti tohoto právního základu, které podporuje analýza Soudního dvora Evropské unie a jeho generálního advokáta v posudku/stanovisku 1/15. V rámci vývoje ohledně platnosti článku 82 jako právního základu pro návrh dohody o jmenné evidenci cestujících (PNR) mezi EU a Kanadou zdůraznil Soudní dvůr, že v případě příslušného kanadského orgánu „se nejedná o justiční ani obdobný orgán“[2]. Zdá se, že v rámci návrhů o elektronických důkazech je jedním z hlavních sledovaných cílů, jak uvádí Komise, vyhnout se „příliš těžkopádné“ justiční spolupráci. Návrh je tudíž založen na zásadě, že by mělo docházet ke spolupráci mezi orgánem a poskytovatelem služeb spíše než mezi dvěma orgány. Předpokládaný postup především staví soukromé subjekty do postavení přijímající strany, která odpovídá na žádosti pocházející od justičních orgánů.

Evropský sbor pro ochranu osobních údajů podotýká, že by proces vymáhání předávacích nebo uchovávacích příkazů mohl implikovat účast přijímajícího orgánu v situaci, kdy přijímající poskytovatel služeb nesplní své povinnosti, a tím vyvolá potřebu požadovat následné vymáhání příkazu. Jelikož však hlavním cílem stanoveného postupu je právě nezapojovat přijímající orgán, má Evropský sbor pro

[2] Viz bod 103 posudku 1/15 a bod 108 stanoviska generálního advokáta v této věci.

ochranu osobních údajů pochybnosti, že by tento doplňkový postup mohl odůvodňovat použití článku 82 jako jediného právního základu nástroje.

Evropský sbor pro ochranu osobních údajů je proto toho názoru, že má-li se článek 82 použít jako právní základ, musí se hlavní procesní kroky spolupráce uskutečnit mezi dvěma justičními orgány a že pro dotyčný druh spolupráce by měl být použit jiný právní základ.

2. Nutnost elektronických důkazů v porovnání se smlouvami o vzájemné právní pomoci a evropským vyšetřovacím příkazem

Evropský sbor pro ochranu osobních údajů podotýká, že se Komise zavázala přezkoumávat překážky trestního vyšetřování, zejména pokud jde o otázku přístupu k elektronickým důkazům. Ve své důvodové zprávě uvádí Komise souvislosti návrhu a zdůrazňuje nestálou povahu elektronických důkazů, jejich mezinárodní rozměr, jakož i potřebu přizpůsobit mechanismus spolupráce digitálnímu věku. Cílem návrhů nařízení a směrnice pro předávání elektronických důkazů a přístup k nim není nahradit předchozí nástroje spolupráce v trestních věcech, jako je Budapešťská úmluva, smlouva o vzájemné právní pomoci a evropský vyšetřovací příkaz (směrnice o evropském vyšetřovacím příkazu). Podle Komise je cílem návrhů o elektronických důkazech zlepšení justiční spolupráce v trestních věcech mezi orgány a poskytovateli služeb na území Unie, jakož i se třetími zeměmi, zejména se Spojenými státy americkými.

Jelikož tyto nové dodatečné nástroje budou konkrétně určeny pro přístup k elektronickým důkazům a jejich předávání, Evropský sbor pro ochranu osobních údajů posoudí přidanou hodnotu nástrojů vzhledem ke směrnici o evropském vyšetřovacím příkazu a smlouvě o vzájemné právní pomoci.

a) Nutnost elektronických důkazů v porovnání se zárukami poskytovanými evropským vyšetřovacím příkazem a smlouvami o vzájemné právní pomoci

Hlavní argument předložený Komisí na podporu návrhů o elektronických důkazech je urychlení procesu zajištění a získání elektronických důkazů, které jsou uloženy a/nebo drženy poskytovateli služeb usazenými v jiné jurisdikci.

Evropský sbor pro ochranu osobních údajů však lituje, že nutnost získat nový nástroj pro zajišťování přístupu k elektronickým důkazům nebyla prokázána v posouzení dopadů. Návrhy totiž neobsahují doklad o tom, že k dosažení cíle návrhů o elektronických důkazech nemohly být použity žádné jiné mírnější prostředky, přičemž mohla být zvažována alternativní řešení. Mohla být například posouzena možnost upravit a zlepšit směrnici o evropském vyšetřovacím příkazu, což by zároveň odpovědělo na zvláštní požadavek podle směrnice o evropském vyšetřovacím příkazu, aby byla posouzena potřeba upravit její znění do 21. května 2019[3]. Jinou možností mohlo být předpokládané použití uchovávacích příkazů k zajištění údajů do vydání formální žádosti založené na smlouvě o vzájemné právní pomoci. Tyto alternativy by umožňovaly zachovat záruky poskytované těmito nástroji a současně by zajistily, že požadované osobní údaje nebudou smazány.

Evropský sbor pro ochranu osobních údajů podotýká, že lhůty stanovené ve směrnici o evropském vyšetřovacím příkazu jsou delší než v návrhu o elektronických důkazech. Vykonávající orgán má totiž

[3] Viz článek 37 směrnice o evropském vyšetřovacím příkazu.

30 dní na to, aby přijal rozhodnutí o uznání žádosti[4], a poté by měl provést příkaz do 90 dní[5]. Evropský sbor pro ochranu osobních údajů se domnívá, že poskytnout v evropském vyšetřovacím příkaze vykonávajícím orgánům 30 dní na uvážení je zásadní záruka, která jim umožňuje posoudit, zda je žádost o vykonání odůvodněná a splňuje všechny podmínky pro vydávání a předávání evropského vyšetřovacího příkazu[6].

Evropský sbor pro ochranu osobních údajů se obává, že desetidenní lhůta uvedená v návrzích o elektronických důkazech pro výkon certifikátu evropského předávacího příkazu (EPOC) bez jakéhokoli času na uvážení brání řádnému posouzení, zda EPOC splňuje všechna kritéria a je správně vyplněn.

Evropský sbor pro ochranu osobních údajů proto doporučuje, aby příjemci EPOC bylo poskytnuto více času na rozhodnutí o tom, zda by příkaz měl nebo neměl být vykonán.

Evropský sbor pro ochranu osobních údajů podotýká, že v případě (certifikátu) evropského uchovávacího příkazu (EPOC-PR) neexistuje žádná záruka, že uchovávání údajů bude omezeno na to, co je nezbytné předat. Doba uchovávání údajů může totiž přesáhnout 60 dní, neboť neexistuje žádná lhůta, ve které má vydávající orgán informovat adresáta, aby upustil od vydání nebo předávací příkaz stáhl. Evropský sbor pro ochranu osobních údajů proto doporučuje alespoň lhůtu, v níž má vydávající orgán upustit od předávacího příkazu nebo jej stáhnout, aby dodržel zásadu minimalizace údajů stanovenou v obecném nařízení o ochraně osobních údajů[7].

Evropský sbor pro ochranu osobních údajů také podotýká, že směrnice o evropském vyšetřovacím příkazu stanoví vrácení důkazů z vydávajícího státu vykonávajícímu orgánu[8]. Návrh nařízení o elektronických důkazech však o takové možnosti mlčí. Co se stane s elektronickými důkazy po jejich předání vydávajícímu orgánu je nejasné.

Evropský sbor pro ochranu osobních údajů proto doporučuje, aby návrh nařízení poskytoval více informací o použití elektronických důkazů po jejich předání vydávajícímu orgánu za účelem splnění obecného nařízení o ochraně osobních údajů a zásady transparentnosti[9], jakož i zásady specifičnosti stanovené smlouvami o vzájemné právní pomoci.

b) Upuštění od zásady oboustranné trestnosti

Evropský sbor pro ochranu osobních údajů potvrzuje, že vzájemné uznávání závisí na uplatňování oboustranné trestnosti, což je způsob, jak si členské státy uchovávají svou svrchovanost. Oboustranná trestnost je však stále více považována za překážku hladké justiční spolupráce. Členské státy EU jsou stále ochotnější spolupracovat i v případech, kdy se vyšetřovací úkony týkají činů, které v jejich vnitrostátním právu nejsou považovány za trestný čin. Evropský sbor pro ochranu osobních údajů však připomíná, že cílem zásady oboustranné trestnosti je poskytnutí další záruky pro zajištění toho, že stát nemůže spoléhat na pomoc jiného státu při uplatňování trestní sankce, která v právním řádu druhého státu neexistuje. To by například bránilo státu žádat o pomoc jiného státu při uvěznění osoby za její politická stanoviska, pokud tato stanoviska nejsou v žádaném státě trestná, nebo při trestním stíhání osoby za podstoupení potratu, pokud tato osoba pobývá v jiném státě, kde to není nezákonné. Zásadu oboustranné trestnosti rovněž často doprovázejí další omezení nebo záruky týkající se sankcí, pokud

[4] Ustanovení čl. 12 odst. 3 směrnice o evropském vyšetřovacím příkazu.
[5] Ustanovení čl. 12 odst. 4 směrnice o evropském vyšetřovacím příkazu.
[6] Článek 6 směrnice o evropském vyšetřovacím příkazu.
[7] Ustanovení čl. 5 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů.
[8] Ustanovení čl. 13 odst. 3 a 4 směrnice o evropském vyšetřovacím příkazu.
[9] Ustanovení čl. 5 odst. 1 písm. a) obecného nařízení o ochraně údajů.

se mezi žádajícím a vykonávajícím státem příliš liší. Hlavním příkladem je závazek neuplatňovat trest smrti v některých smlouvách o vzájemné právní pomoci, pokud neexistuje v právním řádu jedné ze dvou smluvních stran.

Evropský sbor pro ochranu osobních údajů podotýká, že zásada oboustranné trestnosti je v návrhu nařízení o elektronických důkazech vyloučena. Důsledkem však není pouze odstranění obvyklých formalit vzájemného uznávání, ale rovněž odstranění záruk spojených se samotnou zásadou oboustranné trestnosti.

Evropský sbor pro ochranu osobních údajů podotýká, že se skutečně vůbec neodkazuje na právní řád země, kde je usazen žádaný poskytovatel služeb, a že (příkaz k) uchovávání jakýchkoli údajů, jakož i předávání údajů o účastníkovi nebo údajů o přístupu, může být vydán pro všechny trestné činy[10] bez ohledu na to, zda jsou v ostatních členských státech obdobné trestné činy stanoveny nebo nikoli.

Prozatím lze předávací příkazy vydávat a vykonávat pouze za předpokladu, že ve vydávajícím státě je ve srovnatelné vnitrostátní situaci k dispozici obdobné opatření za stejný trestný čin[11]. Kromě toho je, jak Komise vysvětluje v důvodové zprávě návrhu nařízení, stanovena specifičnost údajů o transakcích a údajů o obsahu, neboť jsou považovány za citlivější. Příkazy týkající se údajů o transakcích nebo údajů o obsahu jsou totiž založeny na prahové hodnotě trestu odnětí svobody s horní hranicí sazby nejméně tří let, aby bylo zajištěno dodržování proporcionality a práv dotčených osob[12]. Evropský sbor pro ochranu osobních údajů však zdůrazňuje, že doposud nedošlo v rámci EU k žádné harmonizaci trestných činů trestaných odnětím svobody s horní hranicí sazby nejméně tří let.

Evropský sbor pro ochranu osobních údajů odmítá upuštění od zásady oboustranné trestnosti, jejímž cílem je zajistit, aby stát nemohl spoléhat na pomoc jiných při uplatňování svého vnitrostátního trestního práva mimo území státu, a to od státu, který nesdílí stejný přístup, zejména vzhledem k mizení jiných tradičních významných záruk v oblasti trestního práva (viz bod 3 o kritériích pro umístění a bod 7 písm. g) o možných konfliktech se zákony třetích zemí níže).

c) Důsledek přímého kontaktování společností

Evropský sbor pro ochranu osobních údajů uznává, že elektronické důkazy jsou stále častěji dostupné na soukromé infrastruktuře a mohou se nalézat mimo vyšetřující zemi, ve vlastnictví poskytovatelů služeb.

Evropský sbor pro ochranu osobních údajů podotýká, že po rozhodnutích ve věcech *Yahoo!*[13] a *Skype*[14] v Belgii a v souvislosti s teroristickými útoky je zapotřebí hladší a rychlejší spolupráce mezi veřejnými a soukromými subjekty. V posouzení dopadů odkazuje Komise na tři druhy procesních nástrojů, které zapojují jak orgány veřejné moci, tak poskytovatele služeb. Jsou to justiční spolupráce, přímá spolupráce a přímý přístup. Jestliže první neukládá odpovědnost za vykonání evropského vyšetřovacího příkazu poskytovateli služeb, nýbrž vykonávajícímu orgánu[15], druhá, přímá spolupráce, je založena na spolupráci poskytovatele služeb. Nejrušivější je z pohledu poskytovatele služeb přímý přístup, neboť orgány veřejné moci mají k údajům přístup bez pomoci zprostředkovatele.

[10] Ustanovení čl. 5 odst. 3 a čl. 6 odst. 2 navrhovaného nařízení o elektronických důkazech.
[11] Ustanovení čl. 5 odst. 2 navrhovaného nařízení o elektronických důkazech.
[12] Ustanovení čl. 5 odst. 4 písm. a) navrhovaného nařízení o elektronických důkazech.
[13] Belgický Hof van Cassatie, YAHOO! Inc., č. P.13.2082.N ze dne 1. prosince 2015.
[14] Belgický Correctionele Rechtbank van Antwerpen, afdeling Mechelen, č. ME20.F1.105151-12 ze dne 27. října 2016. (Společnost Skype se proti rozhodnutí odvolala.)
[15] Články 10 až 16.

Evropský sbor pro ochranu osobních údajů se proto obává, že budou-li kontaktováni přímo, poskytovatelé služeb nezajistí ochranu osobních údajů tak účinně, jako jsou schopny a povinny učinit orgány veřejné moci, a zdůrazňuje, že to rovněž povede k nepoužitelnosti určitých procesních záruk pro fyzické osoby, jakož i pro společnosti samotné, předpokládaných v rámci justiční spolupráce[16]. Žádaný poskytovatel služeb by se totiž například musel s cílem napadnout příkaz obrátit na soud jiného (členského) státu, zatímco v rámci justiční spolupráce by jednal s orgány svého vlastního státu. Evropský sbor pro ochranu osobních údajů doporučuje zahrnout do návrhu nařízení další důvody potvrzující, že poskytovatelé služeb budou chránit jednotlivá základní práva, jako je ochrana osobních údajů a respektování soukromého a rodinného života, jakož i informace příslušného úřadu pro ochranu osobních údajů, aby byla zajištěna možnost kontroly.

3. Nový důvod pro právní příslušnost a tzv. mizení kritérií pro umístění

Evropský sbor pro ochranu osobních údajů podotýká, že Komise zdůrazňuje, že jednou z významných změn, které tyto návrhy přinášejí, je mizení kritérií pro umístění a možnost příslušných orgánů podávat žádosti o uchovávání a předávání údajů bez ohledu na to, kde jsou tyto údaje skutečně uloženy.

Z pohledu ochrany údajů není nové, že právní předpis EU o ochraně osobních údajů platí bez ohledu na to, kde jsou údaje dotčených osob uloženy. Použitelnost obecného nařízení o ochraně osobních údajů závisí totiž buď na skutečnosti, že správce nebo zpracovatel je usazen v EU, nebo na tom, zda jsou zpracovávány údaje subjektů údajů z EU, i když správce nebo zpracovatel nejsou usazeni na území EU[17], v kterémžto případě musí rovněž určit právního zástupce v EU[18]. Z pohledu ochrany údajů je důležité uvést, že cílem rozšířené územní působnosti je poskytovat úplnější ochranu subjektům údajů z EU bez ohledu na to, kde je usazena společnost, která jejich údaje zpracovává.

Proto se mizení kritérií pro umístění z pohledu ochrany údajů nejeví jako významná změna, ačkoli v oblasti trestního práva je možná nové. Evropský sbor pro ochranu osobních údajů kromě toho rovněž podotýká, že vazba na území EU je stále zachována, neboť do působnosti návrhů spadají pouze poskytovatelé služeb, kteří v Unii nabízejí služby, a navíc ze skutečnosti, že žádosti lze podávat pouze v souvislosti s trestním vyšetřováním, z čehož vyplývá vazba na EU (buď protože byl trestný čin spáchán na území členského státu, nebo protože byli oběť či pachatel trestného činu občany členského státu).

Pokud by mizení kritérií pro umístění mělo být nyní uplatňováno v trestním právu, týká se nejdůležitější otázka pro Evropský sbor pro ochranu osobních údajů toho, jak zajistit, aby takový vývoj nebyl nepříznivý pro ochranu údajů a procesní práva subjektů údajů a žádaných poskytovatelů služeb v trestním soudním řízení. Z tohoto pohledu Evropský sbor pro ochranu osobních údajů uznává, že v rámci EU byly procesní záruky - přinejmenším částečně - harmonizovány a musí být poskytovány v souladu s Evropskou úmluvou o lidských právech. Lze tedy tvrdit, že mizení kritérií pro umístění by pravděpodobně mělo omezenější důsledky, když jsou důkazy požadovány v rámci EU, v porovnání s opačnou situací, kdy orgány ze třetích zemí žádají o údaje od společností usazených v EU za stejných podmínek, jaké jsou stanoveny v návrhu nařízení o elektronických důkazech. Evropský sbor pro

[16] Z pohledu mezinárodní ochrany údajů viz rovněž „Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes“ (Pracovní dokument o standardech ochrany údajů a soukromí osob v přeshraničních žádostech o údaje pro účely vymáhání trestního práva), Mezinárodní pracovní skupina pro ochranu údajů v telekomunikacích, 63. zasedání, 9. a 10. dubna 2018, Budapešť (Maďarsko).

[17] Viz článek 3, zejména odst. 2.

[18] Viz článek 27.

ochranu osobních údajů se totiž především obává, že to by mohlo vést k problematičtějším situacím. V této souvislosti by orgány ze třetí země, kde platí odlišné a potenciálně menší procesní záruky v oblasti trestního práva, mohly mít přístup k údajům, jež by v EU byly chráněny dalšími zárukami. Z tohoto pohledu Evropský sbor pro ochranu osobních údajů připomíná své obavy ohledně dvojích standardů a oslabení základních práv, jestliže se na poskytovatele služeb a subjekty údajů nevztahují procesní záruky v unijním právu, pokud žádost podá orgán třetí země.

Jelikož tento nový důvod příslušnosti „bez ohledu na umístění údajů" je navíc spojen s postupem, který spoléhá především na přímé žádosti příslušných orgánů adresované poskytovatelům služeb, Evropský sbor pro ochranu osobních údajů se obává, že soukromé společnosti přijímající žádosti, jež nejsou vázány právním nástrojem jako smlouva o vzájemné právní pomoci, kterými se tradičně řídí výměny údajů mezi justičními orgány a jež stanoví záruky, nemusí uplatňovat záruky ochrany osobních údajů. V rámci smluv o vzájemné právní pomoci představují minimální záruky ochrany údajů zejména například povinnosti týkající se mlčenlivosti a zásadu specifičnosti, která znamená, že údaje nebudou zpracovávány pro jiný účel.

Evropský sbor pro ochranu osobních údajů proto připomíná, že v případě, kdy by byl poskytovatel služeb usazen ve třetí zemi bez rozhodnutí o odpovídající úrovni ochrany v této oblasti, by měly být uplatňovány alespoň záruky stanovené ve směrnici (EU) 2016/680, a zejména článek 39, a to i na předávání údajů. Evropský sbor pro ochranu osobních údajů zejména zdůrazňuje, že toto ustanovení předpokládá především informování příslušného úřadu pro ochranu osobních údajů v členském státě vydávajícího orgánu příkazu (příkazů) a dokumentaci předání, a to i co se týče odůvodnění neefektivnosti nebo nevhodnosti předání příslušnému orgánu třetí země.

4. Pojem „poskytovatelé služeb" by měl být omezen nebo doplněn o další záruky práv subjektů údajů

Pokud jde o poskytovatele služeb, Evropský sbor pro ochranu osobních údajů vítá širokou definici, která umožňuje zahrnout komunikační služby i služby „over the top" (OTT), neboť všechny tyto služby jsou funkčně rovnocenné, a proto by předpokládaná opatření mohla mít obdobný dopad na právo na soukromí a právo na důvěrnost komunikací, jak je zdůrazněno v prohlášení WP 29 a dříve ve stanovisku 01/2017 o navrhovaném nařízení o soukromí a elektronických komunikacích. Návrh nařízení o elektronických důkazech se totiž vztahuje na poskytovatele služeb, kteří poskytují služby elektronických komunikací, jak je vymezuje čl. 2 odst. 4 (návrhu) směrnice, kterou se stanoví evropský kodex pro elektronické komunikace, služby informační společnosti, jak je vymezuje čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535, „pro které je uchovávání údajů určující složkou služby poskytované uživateli, včetně sociálních sítí, internetových tržišť umožňujících transakce mezi jejich uživateli a jiných poskytovatelů hostingových služeb", nebo služby číslování IP adres a názvů internetových domén jako „např. poskytovatelé IP adres, registry názvů domén, registrátoři názvů domén a související služby zajištění soukromí a proxy serverů"[19].

Je-li však poskytovatelem služeb ve smyslu návrhu nařízení „jakákoli fyzická nebo právnická osoba, která poskytuje jednu či více z následujících kategorií služeb", obává se Evropský sbor pro ochranu osobních údajů, že by se tento nástroj mohl vztahovat na správce i zpracovatele ve smyslu obecného nařízení o ochraně osobních údajů. „Nabízení služeb", jak je vymezuje čl. 2 odst. 4 návrhu nařízení,

[19] Ustanovení čl. 2 odst. 3 písm. c) navrhovaného nařízení o elektronických důkazech.

totiž zahrnuje jak umožnění právnickým nebo fyzickým osobám v jednom nebo více členských státech využívat vyjmenované služby, tak existenci podstatného spojení s dotyčným členským státem či státy; tyto činnosti zahrnují činnosti prováděné zpracovatelem pro správce, jako například uchovávání údajů.

Proto se Evropský sbor pro ochranu osobních údajů obává, že bez omezení poskytovatelů služeb, kteří jednají jako správci ve smyslu obecného nařízení o ochraně osobních údajů, a bez jakékoli konkrétní povinnosti zpracovatele ohlásit správci údajů, když je mu zaslán předávací nebo uchovávací příkaz, by práva subjektů údajů mohla být obcházena. Je tomu tak zejména proto, že jsou v souvislosti s možnými rozpornými povinnostmi, které adresátovi brání vyplnit obdržené příkazy, justiční orgány v návrhu nařízení samotném rovněž vybízeny, aby kontaktovali nejvhodnější subjekt bez ohledu na příslušná pravidla ochrany údajů, zejména vzhledem k tomu, že by mohly být požadovány jakékoli údaje, nejen osobní údaje, na které se vztahuje obecné nařízení o ochraně osobních údajů[20].

Podle obecného nařízení o ochraně osobních údajů zpracovatel jedná pouze podle pokynů správce. Proto je odpovědností správce zajistit, aby práva subjektů údajů byla dodržována, a poskytnout jim příslušné informace včetně těch, které se týkají příjemců jejich údajů, například v souvislosti s výkonem jejich práva přístupu. Zpracovatel tyto žádosti od subjektů údajů neobdrží a nebude schopen na ně odpovědět, pokud jej o to správce výslovně nepožádá.

Evropský sbor pro ochranu osobních údajů tudíž zdůrazňuje, že nejsou-li jejich práva při uplatňování obecného nařízení o ochraně osobních údajů omezena, subjekty údajů, na které se obecné nařízení o ochraně osobních údajů vztahuje, nemusí být schopny vykonávat účinně svá práva, nemůže-li jim správce poskytnout úplné informace. Evropský sbor pro ochranu osobních údajů rovněž podotýká, že není-li zpracovateli uložena žádná konkrétní povinnost informovat správce, pravděpodobnost neexistence informací je ještě vyšší, když se požadované údaje týkají subjektů údajů, na které se nevztahuje ochrana poskytovaná obecným nařízením o ochraně osobních údajů. Justiční orgány žádající o údaje nebudou mít totiž v tomto případě nutně povinnost informovat subjekty údajů o jejich vlastním dalším zpracování. Evropský sbor pro ochranu osobních údajů proto vyzývá k omezení oblasti působnosti na správce ve smyslu obecného nařízení o ochraně osobních údajů nebo k zavedení ustanovení, které ujasní, že pokud oslovený poskytovatel služeb není správce údajů, musí správce informovat.

5. Pojmy „provozovna" a „právní zástupce" v rámci těchto návrhů by měly být jasně odlišeny od těchto pojmů v rámci obecného nařízení o ochraně osobních údajů

Vzhledem k nepoužitelnosti kritérií lokalizace pro údaje jsou adresáti předávacích a uchovávacích příkazů v působnosti navrhovaného nařízení omezeni na poskytovatele služeb, kteří nabízí služby v Unii, ať jsou usazeni v EU nebo nikoli, s povinností ustanovit právního zástupce podle pravidel navržených v návrhu směrnice. Pojmy „provozovna" a „právní zástupce" jsou tudíž vymezeny v návrzích nástrojů.

Evropský sbor pro ochranu osobních údajů podotýká, že se tyto pojmy vyskytují rovněž v rámci jiných nástrojů EU, zejména v rámci obecného nařízení o ochraně osobních údajů. Mělo by tudíž být uvedeno

[20] Viz čl. 7 odst. 3 a 4.

objasnění definic a vymezení rozdílů mezi těmito pojmy v rámci předloh návrhů a v rámci obecného nařízení o ochraně osobních údajů.

a) Provozovna

Evropský sbor pro ochranu osobních údajů rovněž připomíná, že pojem „provozovna“ v rámci návrhu nařízení nesmí být zaměňován se stejným pojmem v rámci obecného nařízení o ochraně osobních údajů. Pojem „provozovna“, jak jej vymezuje čl. 2 odst. 5 pro účely návrhu nařízení, je totiž chápán šířeji než v obecném nařízení o ochraně osobních údajů, neboť se jím rozumí „buď vlastní výkon hospodářské činnosti po dobu neurčitou prostřednictvím stálé infrastruktury, odkud je prováděna podnikatelská činnost poskytování služeb, nebo stálá infrastruktura, odkud je podnikatelská činnost řízena“ bez ohledu na to, zda v rámci činnosti této provozovny dochází ke zpracování osobních údajů nebo nikoli. Zatímco tedy „provozovnu“ ve smyslu obecného nařízení o ochraně osobních údajů bylo nepochybně nutné zahrnout do pojmu „provozovna“ vymezeného v návrhu nařízení, opačně tomu tak být nemusí.

Evropský sbor pro ochranu osobních údajů proto upozorňuje, že u provozoven poskytovatelů služeb ve smyslu návrhu nařízení to nemusí nutně znamenat, že jsou splněny podmínky pro uplatňování obecného nařízení o ochraně osobních údajů podle čl. 3 odst. 1. V této souvislosti se proto správci a zpracovatelé vyzývají, aby ověřili, zda použitelnost obecného nařízení o ochraně osobních údajů nevyplývá z čl. 3 odst. 2, což by znamenalo jmenování právního zástupce v EU a neexistenci mechanismu jediného kontaktního místa.

b) Právní zástupce

WP 29 ve svém prohlášení zdůraznila, že je nutné se vyvarovat jakékoli záměny mezi povinností jmenovat právního zástupce podle článku 27 obecného nařízení o ochraně osobních údajů a právním zástupcem předpokládaným podle návrhu nařízení o elektronických důkazech.

Když má nyní Evropský sbor pro ochranu osobních údajů předlohu návrhu k dispozici, rád by tato doporučení připomenul, a zejména zdůraznil, že podle jeho názoru musí být právní zástupce ve smyslu návrhu směrnice o jmenování právních zástupců v rámci návrhů o elektronických důkazech v každém případě určen a pověřen konkrétními funkcemi nezávisle na pověření od poskytovatele služeb a musí mít pravomoc odpovídat na žádosti a jednat jménem poskytovatele služeb a silnější odpovědnost než právní zástupce podle obecného nařízení o ochraně osobních údajů.

Evropský sbor pro ochranu osobních údajů navíc zdůrazňuje, že povinnost jmenovat právního zástupce podle předloh návrhů o elektronických důkazech v každém případě, ať je poskytovatel služeb usazen v EU nebo ne, možnost jmenovat dokonce několik právních zástupců pro jednoho poskytovatele služeb podle návrhu směrnice o elektronických důkazech a povinnost oznámit jmenování právního zástupce orgánům členských států se liší od obecného nařízení o ochraně osobních údajů, které takovou povinnost oznámit jmenovaného právního zástupce, výjimky z jmenování a omezenou odpovědnost právního zástupce nestanoví.

Vzhledem k významným rozdílům z hlediska úlohy, odpovědnosti a vztahu k ostatním provozovnám poskytovatele služeb v jednom případě a správci nebo zpracovateli v případě druhém proto Evropský sbor pro ochranu osobních údajů doporučuje, že není-li poskytovatel služeb usazen v EU, ale vztahuje se na něj jak obecné nařízení o ochraně osobních údajů podle čl. 3 odst. 2, tak nařízení o elektronických důkazech, měli by být jmenováni dva různí právní zástupci, každý s jasně odlišnými funkcemi podle nástroje, na jehož základě byl jmenován.

6. Nové kategorie údajů

Navrhované nařízení vymezuje různé kategorie údajů podle článku 2: údaje o účastníkovi, údaje o přístupu, údaje o transakcích a údaje o obsahu. 20. bod odůvodnění návrhu Komise dále stanoví, že: *„Mezi kategorie údajů, které toto nařízení zahrnuje, patří údaje o účastníkovi, údaje o přístupu, údaje o transakcích (tyto tři kategorie jsou označovány jako neobsahové údaje') a údaje o obsahu. Toto rozdělení, kromě údajů o přístupu, existuje v právních předpisech mnoha členských států a též v současném právním rámci USA, který umožňuje poskytovatelům služeb dobrovolné sdílení neobsahových údajů se zahraničními donucovacími orgány."*

Evropský sbor pro ochranu osobních údajů v této souvislosti především zdůrazňuje, že všechny čtyři kategorie údajů uvedené výše je podle právního předpisu EU o ochraně údajů nutno považovat za osobní údaje, neboť obsahují informace, které se týkají identifikované či identifikovatelné fyzické osoby, ať je subjekt údajů v navrhovaném nařízení označován za „účastníka" nebo „uživatele". Obdobně je třeba poznamenat, že „elektronické důkazy", jak je vymezuje čl. 2 odst. 6 návrhu Komise, zahrnují všechny čtyři kategorie údajů, a proto se týkají osobních údajů. Spíše než pravidla pro přístup k důkazům vymezená a kvalifikovaná podle vnitrostátních právních a soudních postupů stanoví proto navrhované nařízení nové hmotněprávní a procesní podmínky týkající se přístupu k osobním údajům.

Zatímco navrhované nařízení stanoví nové podkategorie osobních údajů, pro které platí odlišné procesní podmínky přístupu, Evropský sbor pro ochranu osobních údajů připomíná, že podle příslušné judikatury Soudního dvora EU k prokázání existence zásahu do základního práva na respektování soukromého života není důležité, zda dotyčné informace o soukromém životě představují citlivé údaje nebo zda dotyčné osoby utrpěly případné nepříznivé následky z důvodu tohoto zásahu.

Evropský sbor pro ochranu osobních údajů kromě toho připomíná, že ve vztahu k „neobsahovým údajům", jež podle návrhu Komise zahrnují údaje o účastníkovi, údaje o přístupu a údaje o transakcích, rozhodl Soudní dvůr Evropské unie ve svém rozsudku ve spojených věcech C-203/15 a C-698/15 Tele2 Sverige AB, že na základě metadat, jako jsou údaje o provozu a lokalizační údaje, lze vytvořit profil dotčených osob, který je s ohledem na právo na ochranu soukromého života stejně citlivé povahy, jako je samotný obsah sdělení[21].

Jak již bylo uvedeno v prohlášení WP 29 o aspektech ochrany osobních údajů a soukromí přeshraničního přístupu k elektronickým důkazům ze dne 29. listopadu 2017, Evropský sbor pro ochranu osobních údajů opakuje své pochybnosti a obavy ohledně současného vymezení mezi „neobsahovými údaji" a údaji o obsahu, jakož i ohledně čtyř kategorií osobních údajů stanovených navrhovaným nařízením. Nezdá se totiž, že jsou tyto čtyři navrhované kategorie jasně vymezeny, a definice „údajů o přístupu" je v porovnání s jinými kategoriemi i nadále neurčitá. Evropský sbor pro ochranu osobních údajů proto vyjadřuje politování nad tím, že posouzení dopadů a návrh Komise blíže neodůvodnily zřízení těchto nových podkategorií osobních údajů, a vyjadřuje znepokojení ohledně různé úrovně záruk týkajících se hmotněprávních a procesních podmínek pro přístup ke kategoriím osobních údajů, zejména vzhledem k praktické obtížnosti vyhodnocení, do které kategorie údajů budou požadované údaje v některých případech patřit. Adresy internetových protokolů (dále jen „IP") by například mohly být považovány jak za údaje o transakcích, tak za údaje o účastníkovi.

[21] Rozsudek Soudního dvora ze dne 21. prosince 2016, bod 99.

Evropský sbor pro ochranu osobních údajů v této souvislosti rovněž připomíná, že ve 14. bodě odůvodnění svého návrhu nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích (o soukromí a elektronických komunikacích) Komise vyjadřuje názor, že: „Data elektronických komunikací by měla být definována dostatečně širokým a technologicky neutrálním způsobem, aby zahrnovala veškeré informace týkající se přenášeného nebo vyměňovaného obsahu (obsah elektronických komunikací) a informace týkající se koncového uživatele služeb elektronických komunikací, které jsou zpracovávány pro účely přenášení, šíření nebo umožnění výměny obsahu elektronických komunikací, a to včetně údajů sloužících ke sledování a identifikaci zdroje a cíle komunikace, zeměpisné polohy a data, času, doby trvání a typu komunikace.“ Jelikož se současný i budoucí rámec na ochranu soukromí v elektronických komunikacích, jakož i související omezení práva na soukromí, bude vztahovat na pravidla upravující přístup k elektronickým důkazům pro účely vymáhání práva, Evropský sbor pro ochranu osobních údajů doporučuje, aby do navrhovaného nařízení byla zahrnuta širší definice dat elektronických komunikací s cílem zajistit, aby se vhodné záruky a podmínky pro přístup, jež mají být stanoveny, vztahovaly soustavně jak na „neobsahové údaje“, tak na „údaje o obsahu“.

7. Analýza postupů evropských uchovávacích a předávacích příkazů

Postup adresování předávacího nebo uchovávacího příkazu se jeví zhruba řečeno takto:

- Příslušný justiční orgán – vydávající orgán – vydá v závislosti na typu požadovaných údajů a na druhu příkazu podle (nečetných) podmínek vyjmenovaných v článcích 5 a 6 příkaz a zašle jej za pomoci harmonizovaného certifikátu právnímu zástupci poskytovatele služeb nebo kterékoli jeho provozovně na území EU – adresátovi.
- Po obdržení certifikátu musí adresát příkaz provést, tj. předat údaje do 10 dní nebo – v případě naléhavé situace – do 6 hodin či je uchovávat až po dobu 60 dní, pokud není nemožné tak učinit, protože certifikát je neúplný nebo z důvodů vyšší moci či faktické nemožnosti pro adresáta, nebo protože to adresát odmítne z důvodu rozporných povinností, ať už ve vztahu k základním právům nebo k základním zájmům třetí země nebo na základě jiných důvodů.
- Pokud adresát nesplnil obdržený příkaz, aniž by uvedl důvody akceptované vydávajícím orgánem, jsou předpokládány postupy pro vymáhání příkazů příslušným vymáhajícím orgánem v členském státě, kde je poskytovatel služeb zastoupen nebo usazen, neplatí-li omezené důvody pro odmítnutí a vymáhající orgán nevznese námitky proti uznání nebo vymáhání příkazu.
- Vznesl-li adresát proti příkazu odůvodněnou námitku založenou na rozporných povinnostech, vydávající orgán postoupí věc příslušnému soudu ve svém členském státě, který pak odpovídá za posouzení možného rozporu a za potvrzení oprávněnosti příkazu při neexistenci rozporu. V případě rozporu příslušný soud buď v případě rozporných povinností ve vztahu k základním právům nebo k základním zájmům třetí země kontaktuje ústřední orgány ve třetí zemi prostřednictvím svých vnitrostátních ústředních orgánů s patnáctidenní lhůtou na odpověď, kterou lze na základě odůvodněné žádosti prodloužit o 30 dnů, nebo sám rozhodne, zda oprávněnost příkazu potvrdit nebo příkaz zrušit z jiných důvodů odmítnutí uplatněných adresátem.
- Aniž jsou dotčeny prostředky právní ochrany dostupné podle obecného nařízení o ochraně osobních údajů a směrnice o prosazování práva v souvislosti s ochranou údajů, osoby, jejichž údaje byly získány prostřednictvím předávacího příkazu, musí mít rovněž právo na účinnou právní ochranu proti tomuto příkazu.

Evropský sbor pro ochranu osobních údajů posoudil postupy předpokládané a záruky poskytnuté v návrhu nařízení s cílem ohraničit jednotlivé kroky a ke každému z aspektů uvedenému níže v textu doporučuje následující záruky a změny.

a) Prahové hodnoty pro vydávání příkazů by měly být zvýšeny a příkazy vydávány nebo povolovány soudy

Pokud jde o podmínky vydávání příkazů, Evropský sbor pro ochranu osobních údajů vítá zásadu větších záruk pro přístup k údajům o transakcích nebo o obsahu. Podotýká však, že vzhledem k neexistenci plné harmonizace trestních sankcí mezi členskými státy odkaz na „trestné činy postihnutelné ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let“[22] stále znamená pro subjekty údajů v rámci EU rozdílné prahové hodnoty a rozdíly v ochraně jejich údajů.

Evropský sbor pro ochranu osobních údajů kromě toho zdůrazňuje, že zejména vzhledem k široké definici údajů o účastníkovi se stanovená prahová hodnota zdá být pro uchovávací příkazy a předávací příkazy týkající se údajů o účastníkovi nebo údajů o přístupu dosti nízká, neboť vydání těchto příkazů mohou v zásadě opravňovat všechny trestné činy. Obdobně jsou orgány, které tyto příkazy mohou vydávat, více omezeny v souvislosti s předávacími příkazy týkajícími se údajů o transakcích nebo o obsahu než ohledně vydávání uchovávacích nebo předávacích příkazů pro předávání údajů o účastníkovi nebo o přístupu, neboť státní zástupci mohou vydávat nebo povolovat pouze druhé uvedené příkazy, zatímco vydávat nebo povolovat jakýkoli příkaz může kterýkoli soudce, soud nebo vyšetřující soudce.

Evropský sbor pro ochranu osobních údajů vyjadřuje zejména politování nad tím, že nejnižší prahová hodnota umožňující donucovacím orgánům žádat o přístup k údajům o účastníkovi a přístup k údajům pro jakýkoli trestný čin vychází z *a contrario* výkladu judikatury Soudního dvora Evropské unie (která se zaměřuje na jiné údaje), aby rozlišovala záruky, jež mají být poskytovány. Soudní dvůr totiž konkrétně zdůraznil, že pro údaje o provozu a lokalizační údaje musí být přístup příslušných orgánů omezen výhradně na boj proti závažné trestné činnosti[23]. Evropský sbor pro ochranu osobních údajů by chápal, kdyby návrh stanovil možnost žádat o přístup ke zcela základním informacím, které by umožňovaly pouze identifikovat osobu, aniž by odhalovaly jakékoli údaje o komunikaci, bez předchozího povolení soudu. Vyjadřuje však politování nad širokým *a contrario* výkladem tohoto rozhodnutí Komisí a vyzývá k zavedení vyšších záruk s cílem omezit důvody pro přístup k jiným údajům o účastníkovi a k údajům o přístupu. Evropský sbor pro ochranu osobních údajů navrhuje omezit přístup k těmto údajů buď na seznam trestných činů uvedený v návrhu nařízení, nebo alespoň na „závažné trestné činy“, zejména vzhledem k nižší prahové hodnotě pro předchozí povolení předpokládané pro tyto údaje.

Evropský sbor pro ochranu osobních údajů kromě toho zdůrazňuje, že tento *a contrario* výklad rovněž vede ke skutečnosti, že návrh otevírá státním zástupcům možnost vydávat příkazy nebo povolovat jejich vydávání. Evropský sbor pro ochranu osobních údajů je toho názoru, že kromě žádostí týkajících se zcela základních informací, které by umožňovaly pouze identifikovat osobu, aniž by odhalovaly jakékoli údaje o komunikaci, to představuje krok zpět v porovnání s judikaturou Soudního dvora týkající se přístupu k údajům o komunikacích. Ve své judikatuře týkající se přístupu k údajům o komunikacích pro účely vymáhání práva omezil totiž Soudní dvůr možnost stanovit takový přístup

[22] Viz čl. 5 odst. 3 písm. a).
[23] Viz věc 203/15 – bod (125).

kromě dalších kritérií a *„s výjimkou náležitě odůvodněných naléhavých případů“*[24] na *„předchozí přezkum ze strany soudu nebo nezávislého správního orgánu […] v návaznosti na odůvodněnou žádost (příslušných vnitrostátních orgánů) podanou v rámci postupů pro předcházení, odhalování nebo stíhání trestných činů*.“ [25]

Evropský sbor pro ochranu osobních údajů připomíná, že pojem „soud“ je autonomní pojem unijního práva a že Soudní dvůr neustále zdůrazňuje a připomíná kritéria, která musí být splněna, aby subjekt mohl být kvalifikován jako soud, včetně kritérií nezávislosti[26], což zřejmě není případ státních zástupců, jak připomenul ve své judikatuře rovněž Evropský soud pro lidská práva (ESLP)[27].

Ustanovení čl. 4 odst. 1 písm. a) a b) a odst. 3 písm. a) a b) tedy vedou k postupům, při kterých se na údaje o účastníkovi a o přístupu uplatní podstatně méně záruk, neboť o údaje bude moci žádat státní zástupce sám, bez jakékoli další kontroly orgánů státu, kde se požadované údaje nacházejí, nebo orgánů státu, kde se bude vyskytovat právní zástupce žádané společnosti, ani jakékoli kontroly nezávislého správního orgánu.

Evropský sbor pro ochranu osobních údajů dále bere na vědomí tzv. „doplňkovou záruku“ uvedenou v čl. 5 odst. 2, která omezuje možnost vydat předávací příkaz na případy, že by pro stejný trestný čin bylo ve srovnatelné vnitrostátní situaci ve vydávajícím státě k dispozici obdobné opatření. Varuje však před kontraproduktivním účinkem takového ustanovení: spíše než by poskytovalo doplňkové záruky, vypadá jako pobídka pro členské státy k tomu, aby rozšířily své vnitrostátní možnosti žádat o předání údajů o účastníkovi nebo o přístupu s cílem zajistit, že budou moci být vydávány předávací příkazy podle tohoto nařízení.

b) Lhůty pro poskytnutí údajů by měly být odůvodněné

Evropský sbor pro ochranu osobních údajů podotýká, že na evropské předávací příkazy se musí odpovědět nejpozději do 10 dní po obdržení certifikátu, pokud vydávající orgán neuvede důvody pro dřívější sdělení, a nejpozději do 6 hodin v naléhavých případech, jak uvádí čl. 9 odst. 1 a 2.

Evropský sbor pro ochranu osobních údajů však nezaznamenal žádná kritéria upravující povinnost orgánů doložit naléhavost předání údajů, a to ani následně, s cílem umožnit případnou kontrolu využívání tohoto velmi rychlého postupu, přestože šestihodinová lhůta pravděpodobně znamená velmi zběžnou kontrolu před předáním údajů, ne-li přímo neexistenci jakékoli kontroly ze strany poskytovatele služeb. Posouzení dopadů totiž zdůrazňuje nutnost, aby příslušné orgány měly přístup k údajům včas. Avšak příklady uvedené v posouzení dopadů se všechny týkají důkazů potřebných v případě spáchání závažných trestných činů (případů terorismu s rukojmími, situací probíhajícího pohlavního zneužívání dětí), ale odůvodnění založené na volatilitě důkazů se nezdá být vhodné, pokud neexistuje žádná konkrétní naléhavost kromě této potenciální volatility údajů. Volatilita údajů navíc neposkytuje žádné další odůvodnění ohledně proporcionality přístupu k údajům s méně zárukami v těchto situacích, kdy neexistuje žádná naléhavost kromě volatility údajů.

Evropský sbor pro ochranu osobních údajů kromě toho pochybuje o nutnosti stanovit šestihodinovou lhůtu a zároveň stanovit, že pokud poskytovatel služeb nemůže splnit svou povinnost, tato lhůta by se nepoužila, dokud vydávající orgán neposkytne „do pěti dnů“ další objasnění.

Evropský sbor pro ochranu osobních údajů proto vyžaduje další prvky v posouzení dopadů za účelem odůvodnění nutnosti těchto lhůt v případech, kdy spáchaný nebo stíhaný trestný čin není závažný,

[24] Viz věc 203/15 – bod (120).
[25] Spojené věci C 293/12 a C 594/12, bod (62).
[26] Viz například věc C-203/14.
[27] Viz například Moulin v. Francie ze dne 23. listopadu 2010.

a nejsou-li takové podrobné prvky poskytnuty, výslovná kritéria k odůvodnění naléhavosti v případě vydání certifikátů evropského předávacího příkazu (EPOC). Mohl by být stanoven například stejný model jako ve směrnici o evropském vyšetřovacím příkazu. Směrnice o evropském vyšetřovacím příkazu stanoví kratší lhůtu, je-li odůvodněná „procesními lhůtami, závažností činu nebo jinými zvláště naléhavými okolnostmi“ (viz čl. 12 odst. 2), nebo 24hodinovou lhůtu pro rozhodnutí o předběžných opatřeních (viz čl. 32 odst. 2). Posouzení dopadů návrhu nařízení totiž nestanoví podrobné prvky pro zdůvodnění, proč tyto lhůty nejsou účinné, jediné zdůrazňované prvky jsou, že počet zaslaných žádostí přetěžuje přijímající justiční orgány, jež nemohou dodržet lhůty.

c) Evropské předávací a uchovávací příkazy se nepoužijí k vyžádání údajů o subjektu údajů jiného členského státu, aniž by byly alespoň informovány příslušné orgány dotčeného členského státu, zejména jde-li o údaje o obsahu

Evropský sbor pro ochranu osobních údajů připomíná, že ve stávajících nástrojích je stanovena justiční spolupráce, a tudíž doplňkové záruky, zejména s cílem kontrolovat nutnost a přiměřenost žádostí, a zdůrazňuje, že tyto záruky jsou ještě více odůvodněné v případech, kdy jsou požadovanými údaji údaje o obsahu, jež zahrnují více omezení práv subjektů údajů na ochranu jejich osobních údajů a soukromí. Evropský sbor pro ochranu osobních údajů v tomto ohledu připomíná, že směrnice o evropském vyšetřovacím příkazu rovněž stanoví možnost odposlechu telekomunikačního provozu s technickou pomocí jiného členského státu (viz čl. 30), jakož i povinnost oznámit jakékoli odposlouchávání údajů příslušnému orgánu jiného členského státu, není-li potřeba žádná pomoc, pokud dotčený subjekt údajů je nebo bude na území dotyčného členského stát (viz čl. 31).

Evropský sbor pro ochranu osobních údajů nenalézá žádné odůvodnění pro postup předpokládaný v návrhu nařízení o elektronických důkazech s cílem umožnit předávání údajů o obsahu bez jakékoli účasti alespoň příslušných orgánů členského státu, kde se subjekt údajů vyskytuje.

d) Evropské uchovávací příkazy se nepoužijí k obcházení povinností poskytovatelů služeb uchovávat údaje

Evropský sbor pro ochranu osobních údajů podotýká, že hlavním cílem evropských uchovávacích příkazů je zabránit vymazání údajů.

Ačkoli Evropský sbor pro ochranu osobních údajů uznává, že to v některých případech může být nezbytné a přiměřené, vyjadřuje politování nad nedostatkem záruk týkajících se vydávání těchto příkazů. Evropský sbor pro ochranu osobních údajů zejména doporučuje, že pokud jsou uchovávací příkazy zaměřeny pouze na konkrétní údaje, kde se zdá, že návrh umožňuje široké žádosti, a jsou-li tyto příkazy vydány pro údaje, jejichž vymazání je plánováno v souladu se zásadou uchovávání údajů, příkaz nesmí nikdy sloužit jako základ pro zpracování údajů poskytovatelem služeb po původním datu výmazu. Jinými slovy, údaje by měly být „zmrazeny“.

Kromě toho by vazba mezi uchovávacím příkazem a následnou žádostí o předání údajů, ať už prostřednictvím evropského předávacího příkazu, žádosti evropského vyšetřovacího příkazu nebo žádosti o vzájemnou právní pomoc, měla být posílena s cílem zajistit, aby evropské uchovávací příkazy byly vydávány pouze tehdy, je-li druhá žádost jistá (a nejen zvažovaná jako možnost), a že pokud je

druhá žádost odmítnuta, platnost uchovávacího příkazu rovněž skončí, aniž by se muselo čekat 60 dní[28], je-li následná žádost odmítnuta dříve.

e) Důvěrnost a informace o uživateli

Evropský sbor pro ochranu osobních údajů podotýká, že do návrhu nařízení byl zaveden zvláštní článek[29] týkající se důvěrnosti zaslaných příkazů. Aby se zabránilo nejasnostem a nedorozuměním ohledně práva na ochranu údajů, Evropský sbor pro ochranu osobních údajů připomíná, že ačkoli obecné nařízení o ochraně osobních údajů stanoví, že omezení práv subjektů údajů za účelem zajištění prevence, vyšetřování, odhalování či stíhání trestných činů (trestních sankcí) by mělo být stanoveno zákonem, a proto veřejně přístupné[30], a že tato legislativní opatření musí obsahovat konkrétní ustanovení ohledně práva subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení[31], nestanoví povinnost informovat subjekty údajů jednotlivě o každé žádosti o přístup provedené donucovacími orgány.

Mezitím však Evropský sbor pro ochranu osobních údajů připomíná, že směrnice o ochraně údajů stanoví toto právo subjektů údajů na informace od samotných příslušných orgánů, pokud toto právo nebylo omezeno, a to každého subjektu údajů bez omezení tohoto práva pouze na subjekty údajů s bydlištěm na území EU.

f) Postup vymáhání příkazu, když jej poskytovatel služeb odmítne provést

Evropský sbor pro ochranu osobních údajů podotýká, že článek 14 návrhu nařízení stanoví postup, jak zajistit vymáhání příkazu, když jej adresát neplní, který spoléhá na justiční spolupráci mezi vydávajícím orgánem a příslušným orgánem ve státě vymáhání.

Zdá se však, že tento postup neumožňuje, aby vymáhající orgán odmítl vymáhat předaný příkaz z jiných důvodů než čistě procesních (stejně jako adresát, týkajících se především nedostatku poskytnutých informací nebo faktické nemožnosti poskytnout údaje), protože dotčené údaje jsou podle jeho vnitrostátního práva chráněny imunitou nebo výsadou nebo protože jejich sdělení může mít dopad na jeho základní zájmy jako národní bezpečnost a obrana[32].

Evropský sbor pro ochranu osobních údajů proto opakuje své obavy, pokud jde o odstranění každé opakované kontroly předaného příkazu přijímajícími příslušnými orgány v porovnání s jinými nástroji. Dokonce i důvod odmítnout vymáhat příkaz proto, že by to porušovalo Listinu, se zdá vyšší než klasická prahová hodnota týkající se porušování základních práv dotčených osob. Následování příkladů evropského zatýkacího rozkazu, jenž stanoví povinné, jakož i nepovinné důvody odmítnutí, nebo alespoň směrnice o evropském vyšetřovacím příkazu, která obecně stanoví, že předpoklad, podle kterého „vytvoření prostoru svobody, bezpečnosti a práva v rámci Unie je založeno na vzájemné důvěře a na předpokladu dodržování práva Unie, a zejména základních práv, ze strany ostatních členských států“ je tudíž vyvratitelné[33], návrh nařízení by měl alespoň předpokládat minimální klasickou odchylku, že pokud existují závažné důvody se domnívat, že by vymáhání příkazu vedlo k porušení základního práva dotčené osoby a že vykonávající stát by porušil své povinnosti týkající se ochrany základních práv uznaných v Listině, vymáhání příkazu by mělo být odmítnuto.

[28] Viz čl. 10 odst. 1.
[29] Viz článek 11.
[30] Viz čl. 23 odst. 1 písm. d).
[31] Viz čl. 23 odst. 2 písm. h).
[32] Viz čl. 14 odst. 2.
[33] Viz 19. bod odůvodnění směrnice o evropském vyšetřovacím příkazu.

g) Vymáhání příkazů a rozporné povinnosti podle zákonů třetí země (články 15 a 16)

Evropský sbor pro ochranu osobních údajů vítá možnost odmítnout příkaz z důvodu, že by byl v rozporu se základními právy, stanovenou v návrhu nařízení pro adresáty, neboť jejím cílem je poskytnout záruky v případě rozporných právních povinností. Považuje rovněž za zásadní, že návrh stanoví konzultace orgánů třetích zemí, alespoň když vznikne rozpor, jakož i povinnost zrušit příkaz, pokud orgán třetí země vznese námitku.

Předpokládaný postup odmítnutí provést příkaz z důvodu rozporných povinností podle zákonů třetí země by proto měl být značně zdokonalen.

Evropský sbor pro ochranu osobních údajů za prvé podotýká, že návrh nařízení pověřuje soukromou společnost jako adresáta předávacího příkazu, aby posoudila, zda by dotyčný příkaz byl v rozporu s příslušnými právními předpisy třetí země, které zakazují sdělení žádaných údajů, nebo nikoli. Společnost musí poskytnout odůvodněnou námitku zahrnující všechny relevantní podrobnosti o právu třetí země, jeho použitelnosti v daném případu a povaze rozporné povinnosti.

Evropský sbor pro ochranu osobních údajů se však především obává, že když bude taková námitka vznesena, příslušný soud členského státu vydávajícího orgánu sám posoudí, zda existuje rozpor nebo ne, neboť soud vstoupí do kontaktu s orgány třetí země pouze tehdy, pokud nalezne rozpor. Příslušnému soudu EU je tedy v této souvislosti udělena pravomoc jednoznačně vykládat právo třetí země, aniž by byl specialistou, pokud jde o jeho podstatu. Evropský sbor pro ochranu osobních údajů se domnívá, že povinnost konzultovat příslušné orgány třetí země je proto v současném návrhu příliš omezená. V oblasti ochrany údajů upozorňuje Evropský sbor pro ochranu osobních údajů normotvůrce na skutečnost, že v případě, že by příslušný soud třetí země vykládal obecné nařízení o ochraně osobních údajů, aby posoudil, zda je v rozporu s jeho vlastními požadavky, orgány ochrany údajů EU a příslušné soudy by i nadále měly pravomoc posoudit zákonnost předání na základě rozsudku soudu nebo rozhodnutí správního orgánu třetí země, která požaduje předání nebo sdělení osobních údajů v působnosti obecného nařízení o ochraně osobních údajů[34].

Evropský sbor pro ochranu osobních údajů navíc zdůrazňuje, že posouzení práva třetí země příslušným soudem žádajícího státu EU musí být založeno na objektivních prvcích a vztahují se na něj kritéria, která musí příslušný soud vzít v úvahu při posuzování práva třetí země podle čl. 15 odst. 4 a čl. 16 odst. 5 písm. a) návrhu nařízení. Soud by totiž musel posoudit skutečnost, že „místo toho, aby chránilo základní práva nebo základní zájmy třetí země související s národní bezpečností nebo obranou“, právo třetí země „se očividně snaží chránit jiné zájmy nebo je zaměřeno na ochranu nezákonných činností před žádostmi donucovacích orgánů v kontextu trestního vyšetřování“ nebo „zájem chráněný příslušným právem třetí země, včetně zájmu třetí země na tom, aby se zabránilo sdělení údajů“. Ačkoli by například toto posouzení mělo v zásadě vyžadovat posouzení založené na důkazech s ohledem na všechny dostupné informace vzhledem k možnému dopadu takového rozhodnutí, přinejmenším formulace („is being aimed to“ – je zaměřeno na) se zdá nejasná a měla by být upravena („has the aim/objective to“ – jeho cílem je).

Evropský sbor pro ochranu osobních údajů vyjadřuje politování nad tím, že jediný případ, kdy by byly konzultovány orgány třetí země a mohly by vyslovit námitky vůči vykonání předávacího příkazu, by nastal tehdy, pokud by se tento příslušný soud EU domníval, že existuje relevantní rozpor, a předal všechny prvky ústředním orgánům v dotčené třetí zemi a ústřední orgány dotyčné třetí země by

[34] Viz článek 48 obecného nařízení o ochraně osobních údajů.

vyslovily námitky v těsných lhůtách maximálně 50 dnů (15 dnů případně rozšířených o 30 dnů a po poslední možné připomínce poskytnutí pěti dalších dní). Ve všech ostatních případech by příslušný soud byl schopen potvrdit oprávněnost předávacího příkazu a uložit peněžitou sankci poskytovateli služeb, který odmítá příkaz provést. Evropský sbor pro ochranu osobních údajů se tudíž obává, že příslušné soudy EU nebudou mít širší povinnost konzultovat příslušné orgány dotčených třetích zemí s cílem zajistit, aby postup systematičtěji zabezpečoval, že bude přihlédnuto k argumentům obou stran, a prokázat více respektu vůči právu třetích zemí.

Jak již bylo zdůrazněno v prohlášení pracovní skupiny zřízené podle článku 29 a výše, Evropský sbor pro ochranu osobních údajů připomíná, že by měla být věnována zvláštní pozornost přijímání obdobných nástrojů, jež by mohly ovlivnit práva subjektů údajů a jejich právo na soukromí v rámci EU, třetími zeměmi, zejména riziko obdobných nástrojů, které by vstoupily do přímého rozporu s právními předpisy EU o ochraně údajů.

Evropský sbor pro ochranu osobních údajů kromě toho zdůrazňuje, že příslušný soud členského státu vydávajícího orgánu nemusí ani být příslušným soudem pro vymáhání příkazu předpokládané podle článku 14 návrhu nařízení, což by ještě zvýšilo riziko rozporných postupů a nedostatku křížových kontrol za situace protichůdných právních předpisů. To je důsledkem skutečnosti, že v některých případech by mohly být zapojeny tři státy: stát orgánu, který vydává příkaz, třetí země poskytovatele služeb a členský stát, kde pobývá právní zástupce poskytovatele služeb v EU a kde by příkaz musel být vymáhán. Podle v současnosti předpokládaného postupu by tudíž soud žádajícího orgánu v členském státě A mohl provést svůj vlastní výklad práva třetí země poskytovatele služeb B, aniž by potřeboval názory orgánů této třetí země (zatímco ony by proti příkazu vznesly námitku), a požádat soud jiného členského státu EU C, aby jeho rozhodnutí vymáhal bez jakékoli možnosti vznést námitku.

Evropský sbor pro ochranu osobních údajů mimo to rovněž vítá zavedení specifických opravných prostředků proti předávacím příkazům kromě opravných prostředků stanovených v obecném nařízení o ochraně osobních údajů a ve směrnici o prosazování práva v souvislosti s ochranou údajů. Pracovní skupina zřízená podle článku 29 takové záruky požadovala již ve svém předchozím prohlášení. Evropský sbor pro ochranu osobních údajů však lituje, že takové opravné prostředky nejsou rovněž předpokládané proti uchovávacím příkazům, neboť tyto příkazy mohou rovněž vést k omezením základních práv fyzických osob, jejichž údaje jsou uchovávány. Uchovávací příkazy mohou totiž způsobit, že jsou údaje uchovávány déle, než by byly podle pravidel ochrany údajů. Uchovávací příkaz proto sám o sobě vede k omezení základních práv dotčeného subjektu údajů a jeho odůvodnění musí podléhat přezkumu a specifickým opravným prostředkům, zejména v případech, kdy bude uchovávací příkaz vydán souběžně s předávacím příkazem s cílem údaje získat. Jak doporučila pracovní skupina zřízená podle článku 29 ve svém prohlášení, měly by být předpokládány opravné prostředky alespoň rovnocenné těm, které jsou dostupné ve vnitrostátním případě.

h) Bezpečnost předávání údajů při odpovědi na příkaz

Evropský sbor pro ochranu osobních údajů podotýká, že návrh nařízení upravuje pouze příkazy, jež mají být adresovány příjemcům na území Evropské unie, a proto nestanoví žádný konkrétní kanál pro předávání údajů mezi adresáty a poskytovateli služeb sídlícími mimo Evropskou unii.

Ačkoli Evropský sbor pro ochranu osobních údajů vítá neexistenci dalších odchylek od obecného rámce EU pro ochranu údajů, připomíná, že každý příkaz zaslaný adresátovi, který by poté znamenal předání mimo EU, by musel dodržet právní rámec stanovený obecným nařízením o ochraně osobních údajů. Obcházení právního rámce justiční spolupráce, který stanoví záruky ochrany údajů, jež mají být dodržovány, by nemělo vést také k obcházení požadavků na předávání údajů adresáty předávacích nebo uchovávacích příkazů s cílem splnit tyto příkazy.

I když Evropský sbor pro ochranu osobních údajů vítá neexistenci ustanovení ukládajícího povinnost dekódovat kódované údaje[35], obává se, že předlohy návrhů nepředpokládají žádný zvláštní požadavek na adresáty, aby posoudili pravost předaných údajů, zdůrazňuje, že toto posouzení je rovněž přidanou hodnotou tradičních nástrojů spoléhajících na justiční spolupráci, a varuje před zvýšenými riziky pro dotčené subjekty údajů, které z neexistence takového posouzení vyplývají.

Závěry

Na základě tohoto posouzení hodlá Evropský sbor pro ochranu osobních údajůučinit společným normotvůrcům tato doporučení:

1) Právním základem nařízení by neměl být čl. 82 odst. 1 SFEU.
2) Nutnost nového nástroje v porovnání se stávající směrnicí o evropském vyšetřovacím příkazu nebo smlouvou o vzájemné právní pomoci by měla být lépe prokázána, a to i pomocí podrobné analýzy mírnějších prostředků ve vztahu k základním právům, jako jsou změny uvedených stávajících nástrojů nebo omezení oblasti působnosti tohoto nástroje na uchovávací příkazy v kombinaci s jinými stávajícími postupy vyžádání přístupu k údajům.
3) Nařízení by mělo stanovit delší lhůtu, aby vykonávajícímu poskytovateli služeb umožňovalo zajistit, že záruky ve vztahu k ochraně základních práv lze dodržet.
4) Zásada oboustranné trestnosti by měla být zachována, zejména pokud jsou opuštěna kritéria pro umístění údajů, aby byla zachována povinnost přihlédnout k zárukám poskytovaným v obou dotčených státech (ve státě žádajícího orgánu a ve státě, kde sídlí poskytovatel služeb).
5) Oblast působnosti nařízení by měla být omezena na správce ve smyslu obecného nařízení o ochraně osobních údajů nebo by zařízení mělo zahrnovat ustanovení, že pokud oslovený poskytovatel služeb není správce údajů ale zpracovatel, je povinen informovat správce.
6) Nařízení by mělo zahrnovat záruky týkající se předávání údajů v případě, že by poskytovatel služeb byl usazen ve třetí zemi bez rozhodnutí o odpovídající úrovni ochrany v této oblasti, nebo odkazovat na směrnici (EU) 2016/680, neboť tyto záruky budou použitelné.
7) Jelikož se povinné jmenování právního zástupce liší od obecného nařízení o ochraně osobních údajů, nařízení by mělo upřesnit, že právní zástupce jmenovaný podle nařízení o elektronických důkazech by měl být odlišný od zástupce jmenovaného podle čl. 3 odst. 2 obecného nařízení o ochraně osobních údajů.

[35] Viz 19. bod odůvodnění a strana 240 posouzení dopadů.

8) Nařízení by mělo obsahovat širší definici údajů elektronických komunikací s cílem zajistit, aby se vhodné záruky a podmínky pro přístup, jež mají být stanoveny, vztahovaly jak na neobsahové údaje, tak na údaje o obsahu.
9) Nařízení by mělo zvýšit prahové hodnoty pro vydávání příkazů a příkazy musí být vydávány nebo povolovány soudy s výjimkou údajů o účastníkovi za předpokladu, že definice této kategorie údajů se drasticky zúží na zcela základní informace, které umožňují pouze identifikovat osobu, aniž by zahrnovaly přístup k jakýmkoli údajům o komunikaci.
10) Nařízení by mělo omezit přístup k údajům o účastníkovi a o přístupu na přísně stanovený seznam trestných činů nebo alespoň na „závažné trestné činy".
11) Lhůta pro poskytnutí údajů, zejména v případě naléhavé situace, by měla být v nařízení lépe odůvodněna a možnost využít rychlého šestihodinového postupu by měla zahrnovat povinnost žádajících orgánů doložit naléhavost, která byla podnětem k použití tohoto postupu, a to i následně, aby se umožnila kontrola používání takových výjimečných pravomocí.
12) Postup umožňující předávání údajů o obsahu bez jakékoli účasti příslušných orgánů členského státu, ve kterém se subjekt údajů vyskytuje, by měl být opuštěn.
13) Záruky týkající se vydávání evropských uchovávacích příkazů by měly být v nařízení zdokonaleny.
14) Nařízení by mělo zahrnovat alespoň minimální klasickou odchylku, že existují-li závažné důvody se domnívat, že by vymáhání příkazu vedlo k porušení základního práva dotčené osoby a k tomu, že by vykonávající stát porušil své povinnosti týkající se ochrany základních práv uznaných v Listině, vymáhání příkazu by mělo být odmítnuto.
15) Nařízení by mělo předpokládat širší povinnost konzultovat v případě kolize norem příslušné orgány třetí země, kde sídlí poskytovatel služeb, od kterého se žádá, aby poskytl údaje, aby se zabránilo subjektivním výkladům jediného soudu.
16) Platnost a doba trvání uchovávacích příkazů by měla být více vázána na předávací příkazy, které je doprovázejí.
17) Bezpečnost předávání údajů by měla být lépe zaručena.
18) Mělo by být předpokládáno ověření pravosti údajů, zejména pokud by mohly být poskytovány kódované údaje.

Za Evropský sbor pro ochranu osobních údajů

Předsedkyně

(Andrea Jelinek)